(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－18148
（P2003－18148A）
(43)公開日　平成15年１月17日(2003.1.17)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）	
H04L	9/08		H04L	9/00	601C	5J104
H04B	7/26		H04B	7/26	M	5K002
	10/00			9/00	A	5K067
	10/22		H04L	9/00	675A	
H04L	9/32		H04B	7/26	109R	

審査請求 有　請求項の数12　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願2001－204889(P2001－204889)

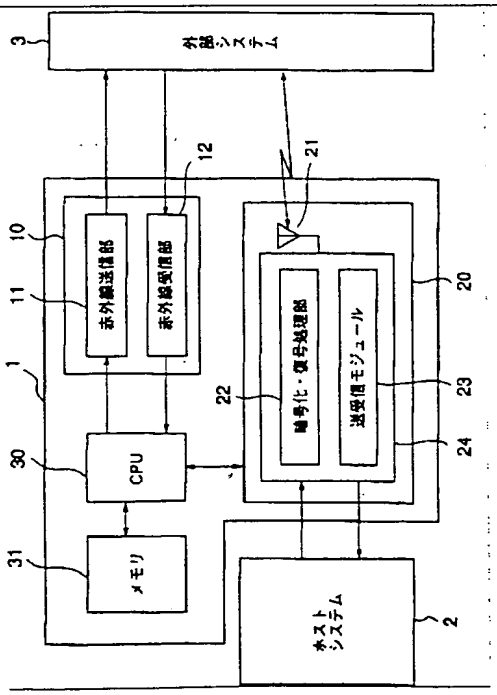
(22)出願日　平成13年７月５日(2001.7.5)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　木下　雄弘
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5J104 AA03 AA16 EA04 EA21 NA02 PA02
5K002 AA05 DA05 FA03 GA07
5K067 AA33 BB21 EE35 EE37 HH36

(54)【発明の名称】　無線データ通信装置及びそのデータ通信方法

(57)【要約】
【課題】共有鍵方式のセキュリティ機能に必要なキー情報の秘匿性を十分に確保できる無線データ通信装置を提供することにある。
【解決手段】Ｂｌｕｅｔｏｏｔｈ無線通信方式を採用する無線データ通信装置において、認証処理や暗号化処理に使用する共有キー情報を赤外線通信部１０を使用して交換する。ＣＰＵ３０は、交換した共有キー情報をメモリ３１に記憶し、認証処理及び暗号化・復号化処理部２２の暗号化・復号化キー情報の生成処理に使用する。無線データ通信部２０は、暗号化・復号化処理部２２により暗号化されたデータを送信し、また受信データの復号化を実行する。



【特許請求の範囲】
【請求項１】　データの暗号化処理を実行する暗号化手段と、
相手局との間で暗号化データの送受信を行なう無線データ通信手段と、
前記暗号化手段での暗号化処理に必要なキー情報を前記相手局との間で交換するキー情報通信手段とを具備したことを特徴とする無線データ通信装置。
【請求項２】　前記キー情報通信手段は、赤外線通信方式によりデータ通信を実行する赤外線通信手段であることを特徴とする請求項１記載の無線データ通信装置。
【請求項３】　前記無線データ通信手段を使用して、データ通信を行なう相手局との接続に必要な手順を実行する手段を有することを特徴とする請求項１または請求項２のいずれか１項に記載の無線データ通信装置。
【請求項４】　前記キー情報通信手段で交換したキー情報を登録し、当該キー情報を使用してデータ通信を行なう相手局の認証処理を実行する手段を有することを特徴とする請求項１から請求項３のいずれか１項に記載の無線データ通信装置。
【請求項５】　前記キー情報通信手段は、前記無線データ通信手段とは異なる無線通信方式によるデータ通信を実行する無線通信手段であることを特徴とする請求項１記載の無線データ通信装置。
【請求項６】　電子機器に設けられる回路モジュールであって、
前記電子機器で処理されるデータの暗号化処理を実行する暗号化モジュールと、
相手局との間で暗号化データの送受信を行なう無線データ通信モジュールと、
前記無線データ通信モジュールとは異なる無線通信方式により、前記暗号化モジュールでの暗号化処理に必要なキー情報を相手局との間で交換する通信モジュールとを具備したことを特徴とする回路モジュール。
【請求項７】　前記通信モジュールは、赤外線通信モジュールから構成されていることを特徴とする請求項６記載の回路モジュール。
【請求項８】　前記通信モジュールは、セルラー電話モジュールから構成されていることを特徴とする請求項６記載の回路モジュール。
【請求項９】　前記電子機器に対して着脱自在なカードモジュールから構成されていることを特徴とする請求項６から請求項８のいずれか１項に記載の回路モジュール。
【請求項１０】　前記通信モジュールで交換したキー情報を登録し、当該キー情報を使用してデータ通信を行なう相手局の認証処理を実行する手段を有することを特徴とする請求項６から請求項９のいずれか１項に記載の回路モジュール。
【請求項１１】　データ通信を行なうための無線データ通信装置に適用するデータ通信方法であって、
相手局との間で、データの暗号化処理に必要なキー情報を赤外線通信手段により交換するステップと、
前記キー情報を使用してデータの暗号化処理を実行するステップと、
暗号化データの送受信を無線データ通信手段により実行するステップとを有することを特徴とする無線データ通信装置。
【請求項１２】　前記無線データ通信手段を使用して、データ通信を行なう相手局との接続に必要な手順を実行するステップと、
前記赤外線通信手段で交換したキー情報を登録し、当該キー情報を使用してデータ通信を行なう相手局の認証処理を実行するステップとをさらに有することを特徴とする特徴とする請求項１１記載のデータ通信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、一般的には無線データ通信装置に関し、特にセキュリティ技術の改善に関する。
【０００２】
【従来の技術】近年、各種の電子機器の間で、例えばＢｌｕｅｔｏｏｔｈと呼ばれる無線通信方式による近距離のデータ通信を可能とする技術が開発されている。各種の電子機器としては、パーソナルコンピュータ以外に、例えばＰＤＡ（Personal Digital Assistant）と呼ばれる携帯情報端末、セルラー電話機（携帯電話機）、携帯型オーディオ機器、あるいはデジタルカメラなどが含まれる。
【０００３】これらの電子機器間で、無線データ通信が可能であれば、ケーブルによる接続が不要になるなどの利便性を向上できる。このような機能を実現するために、電子機器に対して着脱可能なＩＣカードや、機器の内部に設けるチップセット（ＩＣ回路モジュール）から構成される無線データ通信装置（無線通信デバイス）が開発されている。
【０００４】ところで、無線データ通信では、相手局（無線通信デバイスを含む相手側電子機器）との間で交換するデータを保護するためのセキュリティ機能が重要である。例えばＢｌｕｅｔｏｏｔｈ無線通信方式では、セキュリティ機能として、認証機能と暗号化（復号化を含む）機能の規格が提案されている。いずれの機能も、共有鍵方式と呼ばれる鍵情報（以下キー情報と呼ぶ）の交換を伴う方式が採用されている。即ち、特定の相手局との接続の可否を判断する認証処理、及び通信中のデータを第三者から保護するための暗号化処理のいずれの場合でも、共有するキー情報を使用するセキュリティ方式である。
【０００５】
【発明が解決しようとする課題】例えばＢｌｕｅｔｏｏ

ｔｈ無線通信方式を採用した無線データ通信では、相手局との間でキー情報を共有（交換）し、当該キー情報を使用して認証処理や暗号化処理を行なうセキュリティ方式が採用されている。

【０００６】Ｂｌｕｅｔｏｏｔｈ無線通信方式では、セキュリティ機能は、リンクキー（link key）という概念により管理されている。リンクキーは、ある特定の通信端末間のセキュリティを管理するパラメータ情報であり、データベースに登録されて使用される。このリンクキー（即ち、キー情報）の秘匿性が、無線データ通信におけるセキュリティ機能の強度に大きく影響する。要するに、無線データ通信を開始する際に、セキュリティ機能に必要なキー情報を第三者から確実に保護することが必要である。しかしながら、従来では、相手局と共有するキー情報を無線通信により交換する方式が採用されているため、秘匿性の確保が必ずしも十分とはいえない。

【０００７】そこで、本発明の目的は、共有鍵方式のセキュリティ機能に必要なキー情報の秘匿性を十分に確保できる無線データ通信装置を提供することにある。

【０００８】

【課題を解決するための手段】本発明は、例えばＢｌｕｅｔｏｏｔｈ無線通信方式を採用する無線データ通信装置において、共有キー情報を使用して認証処理や暗号化処理を行なうセキュリティ方式に関し、通常のデータ通信（ユーザデータの通信）に使用する無線通信規格とは異なる無線通信方式により、当該共有キー情報の通信を実行する無線データ通信装置である。

【０００９】具体的には，本発明の装置は、データの暗号化処理を実行する暗号化手段と、相手局との間で暗号化データの送受信を行なう無線データ通信手段と、暗号化手段での暗号化処理に必要なキー情報を相手局との間で交換するキー情報通信手段とを備えたものである。当該キー情報通信手段は、無線データ通信手段の無線通信規格とは異なる無線通信方式であり、具体的には赤外線通信方式を採用した通信手段である。

【００１０】このような構成により、無線データ通信手段によるデータ通信を実行する前段階のセキュリティ手順として、相手局との間でキー情報を共有するために、当該キー情報を赤外線通信方式等のキー情報通信手段により交換する。換言すれば、通常のデータ通信方式と、セキュリティ機能に必要なキー情報の通信方式とを分離する。これにより、同一の通信方式による通信と比較して、通信中のキー情報の秘匿性を十分に確保することが可能となる。従って、共有するキー情報を使用するセキュリティ機能の強度を向上させることができるため、結果としてデータ通信の信頼性を向上させることが可能となる。

【００１１】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【００１２】（無線データ通信装置及びシステムの構成）図１は、同実施形態に関する無線データ通信装置及び通信システムの構成を示すブロック図である。

【００１３】同実施形態では、無線データ通信装置（以下無線通信デバイスと表記する）１は、ＰＤＡなどの情報端末等の電子機器を意味するホストシステム２に対して着脱可能なＩＣカード、または当該システム２に内蔵されるチップセットＩＣ（回路モジュール）から構成される。更に、同実施形態では、ホストシステム２が、当該無線通信デバイス１を介して、外部システム（以下相手局と表記する）３との間でデータ通信を行なう通信システムを想定する。ここで、相手局３とは、当該無線通信デバイス１と同様の仕様のデバイスを有する電子機器である。

【００１４】無線通信デバイス１は、メイン要素である無線データ通信部２０とは別に、キー情報交換部として機能する赤外線通信部１０を有する。赤外線通信部１０は、通常のＩｒＤＡ（Infrared Data Association）規格による赤外線データ通信を実行するモジュールであり、赤外線送信部１１と赤外線受信部１２とから構成されている。

【００１５】無線データ通信部２０、マイクロプロセッサ（ＣＰＵ）３０、及びメモリ３１は、Ｂｌｕｅｔｏｏｔｈ無線通信方式によるデータ通信機能を実現するモジュールである。無線データ通信部２０は、大別して送受信用のアンテナ２１と、暗号化・復号化処理部２２と、送受信モジュール２３とを有する。送受信モジュール２３は、無線データ通信機能を実現するために、無線通信コントローラ、高周波処理部、ベースバンド処理部、及びＩ／Ｏ処理部等の要素を有する。暗号化・復号化処理部２２は、Ｂｌｕｅｔｏｏｔｈ無線通信方式でのキー情報（リンクキー）を使用して、送信データの暗号化処理及び受信データの復号化処理を実行するモジュールである。

【００１６】ＣＰＵ３０は、Ｂｌｕｅｔｏｏｔｈ無線通信方式によるデータ通信及びセキュリティ処理の制御を実行する。メモリ３１は、セキュリティ処理におけるキー情報（リンクキー）を記憶する例えばフラッシュＥＥＰＲＯＭからなる。

【００１７】（システムの概略的動作）以下図４のフローチャート及び図７のタイミングチャートを参照して、同実施形態の無線通信デバイス１によるデータ通信システムの概略的動作を説明する。

【００１８】まず、ＣＰＵ３０は、ホストシステム２からの指示に従って、無線データ通信部２０を起動して、自局と相手局３間のデータ通信を行なうための一連の手順（詳細は後述する）を実行する（ステップＳ２１）。具体的には、無線データ通信部２０のアンテナ２１及び送受信モジュール２３により、相手局３と交信して、キー情報の交換に必要な赤外線通信部１０に相当する通信

手段を備えているか否かを確認する（ステップＳ２２）。即ち、図７の７０に示すように、相手局３の属性に含まれる赤外線通信部１０に相当する通信機能を備えているか否かを問い合わせる。自局側であるＣＰＵ３０は、相手局３からの回答により、赤外線通信部１０に相当する通信手段を備えていることを確認する（７１）。

【００１９】ＣＰＵ３０は、赤外線通信部１０の赤外線送信部１１及び赤外線受信部１２を通じて、図７の７２に示すように、相手局３との間でセキュリティ機能に必要なキー情報（後述するリンクキー）を交換する（ステップＳ２３）。ＣＰＵ３０は、交換（共有）したキー情報をメモリ３１に記憶（データベースへの登録）する（ステップＳ２４）。

【００２０】次に、ＣＰＵ３０は、ホストシステム２からのデータ通信要求に応じて、メモリ３１からキー情報を読出して、暗号化・復号化処理部２２に引き渡す。暗号化・復号化処理部２２は、キー情報を使用して、ホストシステム２からの送信データを暗号化処理して送受信モジュール２３に転送する（ステップＳ２５）。ここで、図７の７３及び７４に示すように、自局と相手局３のそれぞれは、交換したキー情報を使用して、相互の認証処理及び暗号化・復号化に必要なキー情報の生成処理を実行する。

【００２１】暗号化・復号化処理部２２は、生成したキー情報を使用して、送信データの暗号化及び受信データの復号化の処理を実行する。これにより、自局と相手局３間は、図７の７５に示すように、暗号化データの交信を行なう。即ち、送受信モジュール２３は、暗号化データをアンテナ２１を介して相手局３に送信する。また、暗号化・復号化処理部２２は、キー情報を使用して、送受信モジュール２３により相手局３からの受信データを復号化処理してホストシステム２に転送する（ステップＳ２５）。

【００２２】（セキュリティ機能を有するデータ通信動作）以下図２及び図３のフローチャートを参照して、同実施形態の無線通信デバイス１において、特にＢｌｕｅｔｏｏｔｈ無線通信方式によるデータ通信及びセキュリティ処理の手順を説明する。

【００２３】Ｂｌｕｅｔｏｏｔｈ無線通信方式でのセキュリティ方式は、データ通信の接続要求に応じて、リンクキー（キー情報）を使用して認証処理を実行し、認証された場合に当該リンクキーを使用して暗号化・復号化処理に必要なキー情報を生成する手順を実行する（図３のフローチャートを参照）。

【００２４】同実施形態では、当該セキュリティ手順の前段階として、ＣＰＵ３０は、赤外線通信部１０を使用して、相手局３との間でキー情報を交換（共有）する処理を実行する。ここで、ＣＰＵ３０は、Ｂｌｕｅｔｏｏｔｈ規格に含まれるＳＤＰ（Service Discovery Protocol）による問い合わせ処理（SDP-Service Search Request）を利用して、相手局３の属性に含まれる赤外線通信部１０に相当する通信機能を備えているか否かを確認する（ステップＳ１）。

【００２５】ＣＰＵ３０は、無線データ通信部２０のアンテナ２１及び送受信モジュール２３を介して相手局３にＳＤＰによる問い合わせを実行し、相手局３からの問い合わせ応答を待つ（ステップＳ２）。具体的には、相手局３は、赤外線通信部１０に相当する通信機能を備えているという属性を示すパケット（SDP-Service Search Response）を送信する。ＣＰＵ３０は、相手局３からの問い合わせ応答により、赤外線通信部１０によるデータ通信が可能であることを確認する（ステップＳ３のＹＥＳ）。次に、ＣＰＵ３０は、赤外線送信部１１を通じて呼び出し処理（page）を実行することにより、相手局３との通信接続の確立を図る（ステップＳ４）。具体的には、ＣＰＵ３０は、ＩＤパケットを送信し、相手局３からの呼び出し応答（page response）を赤外線受信部１２を通じて受信すると、通信接続フェーズへ移行する（ステップＳ５のＹＥＳ）。

【００２６】このような相手局３との交信により、ＣＰＵ３０は、相手局３との間で赤外線通信部１０によるデータ通信接続を確立し、セキュリティ機能に必要なキー情報の交換（共有）を実行し、メモリ３１に記憶する（図４のフローチャートを参照）。

【００２７】次に、図３のフローチャートを参照して、同実施形態のセキュリティ手順を説明する。

【００２８】まず、Ｂｌｕｅｔｏｏｔｈ方式のセキュリティ手順としては、リンクキーの登録がなされているか否かが判断される（ステップＳ１０）。同実施形態では、相手局３との間で赤外線通信部１０により交換したキー情報をリンクキーとして利用する。即ち、ＣＰＵ３０は、メモリ３１に記憶されているキー情報を、データベースに登録されたリンクキーとして利用する。

【００２９】なお、通常のＢｌｕｅｔｏｏｔｈ方式のセキュリティ手順として、初期時には、リンクキーはデータベースには登録されていないため、初期化キーと称する暫定リンクキーの生成処理が実行される（ステップＳ１０のＮＯ）。初期時には、当該初期化キーによる認証処理が実行される。この初期キーの生成では、各端末（電子機器）で個別に入力されるＰＩＮコードと、内部で発生される乱数データとがパラメータとして使用される。この乱数データは、相互に通信されて共有される。

【００３０】ＣＰＵ３０は、データベースに登録されているリンクキーとして、メモリ３１に記憶された共有キー情報を利用して、相手局３の認証処理を実行する（ステップＳ１１）。この認証処理により確認されると、ＣＰＵ３０は、当該リンクキー（共有キー情報）を使用して、暗号化・復号化キー情報を生成し、暗号化・復号化処理部２２に引き渡す（ステップＳ１３）。

【００３１】ホストシステム２からデータ送信の要求が

あると、暗号化・復号化処理部２２は、暗号化・復号化キー情報を使用して、ホストシステム２からの送信データを暗号化処理する（ステップＳ１４のＹＥＳ，Ｓ１５）。送受信モジュール２３は、暗号化データをアンテナ２１を介して相手局３に送信する（ステップＳ１６）。

【００３２】一方、送受信モジュール２３が相手局３からデータを受信すると、暗号化・復号化処理部２２は、暗号化・復号化キー情報を使用して受信データを復号化処理する（ステップＳ１７，Ｓ１８）。暗号化・復号化処理部２２は、復号化した受信データをホストシステム２に転送する。

【００３３】以上のように同実施形態の無線データ通信方式によれば、データ通信を実行する前段階のセキュリティ手順として、相手局との間でセキュリティ機能に必要なキー情報（リンクキーとして利用）を共有するために、当該キー情報を赤外線通信部１０により交換する。要するに、通常のデータ通信とは異なる無線通信方式により、セキュリティ機能に必要なキー情報の通信を行なう。従って、無線データ通信部２０を使用する通信方式と比較して、通信中のキー情報の秘匿性を十分に確保することが可能となる。従って、共有するキー情報を使用するセキュリティ機能の強度を向上させることができるため、結果としてデータ通信の信頼性を向上させることが可能となる。

【００３４】（変形例）図５及び図６は、同実施形態の変形例に関する図である。

【００３５】本変形例は、図５に示すように、キー情報交換部として、赤外線通信部１０の代わりに、セルラー電話装置（携帯電話機）５０を利用する無線データ通信装置１である。要するに、キー情報交換部は、無線データ通信部２０と異なる無線通信方式の通信装置である。

【００３６】本変形例の場合でも、赤外線通信部１０の代わりにセルラー電話装置５０を利用する点が異なるだけで、基本的な動作は同実施形態と同様である。即ち、図６のフローチャートに示すように、セキュリティ手順の前段階として、ＣＰＵ３０は、セルラー電話装置５０を使用して、相手局３との間でキー情報を、前述したＳＤＰによる問い合わせ処理を利用して、相手局３の属性に含まれるセルラー電話通信機能を備えているか否かを確認する（ステップＳ６０）。ＣＰＵ３０は、相手局３からの問い合わせ応答により、セルラー電話装置５０によるデータ通信が可能であることを確認する（ステップＳ６１，Ｓ６２）。次に、ＣＰＵ３０は、セルラー電話装置５０を通じて呼び出し処理を実行することにより、相手局３との通信接続の確立を図る（ステップＳ６３）。具体的には、ＣＰＵ３０は、ＩＤパケットを送信し、相手局３からの呼び出し応答をセルラー電話装置５０を通じて受信すると、通信接続フェーズへ移行する（ステップＳ６４のＹＥＳ）。

【００３７】なお、図５に示すセルラー電話装置５０以外の各構成要素は、図１に示す同一符号の構成要素の機能と同様である。また、セキュリティ処理の手順は、同実施形態の図３のフローチャートで示すものと同様である。

【００３８】

【発明の効果】以上詳述したように本発明によれば、共有鍵方式のセキュリティ機能に必要なキー情報を、通常のデータ通信（ユーザデータの通信）に使用する無線通信規格とは異なる無線通信方式により交換する。従って、通信中のキー情報の秘匿性を十分に確保できる。これにより、共有するキー情報を使用するセキュリティ機能の強度を向上させることができるため、結果として信頼性の高い無線データ通信機能を実現することができる。

【図面の簡単な説明】

【図１】本発明の実施形態に関する無線データ通信装置及びデータ通信システムの構成を示すブロック図。

【図２】同実施形態に関する無線データ通信装置の接続動作を説明するためのフローチャート。

【図３】同実施形態に関する無線データ通信装置のセキュリティ動作を説明するためのフローチャート。

【図４】同実施形態に関するシステムの概略的動作を説明するためのフローチャート。

【図５】同実施形態の変形例に関するブロック図。

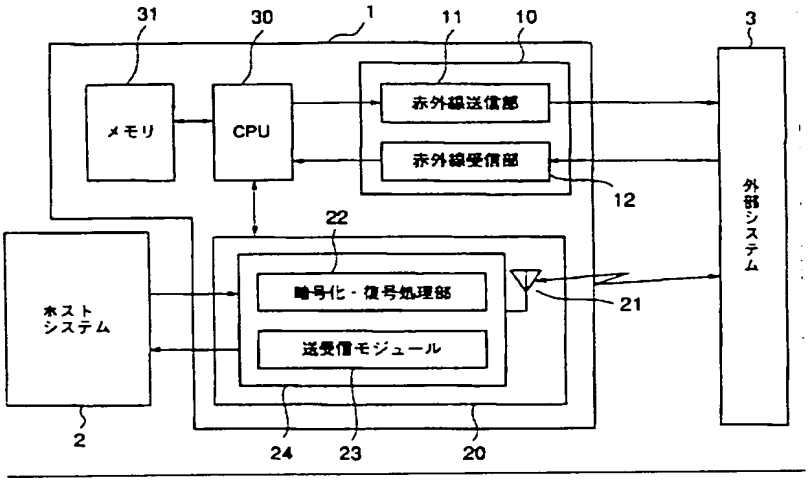
【図６】同変形例に関する無線データ通信装置の接続動作を説明するためのフローチャート。

【図７】同実施形態に関するシステムの概略的動作を説明するためのタイミングチャート。

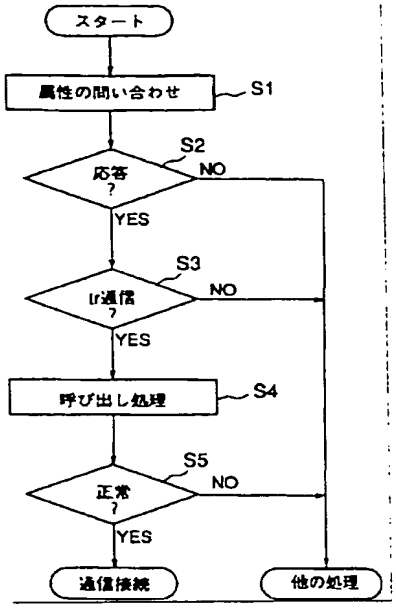
【符号の説明】

１…無線データ通信装置（無線通信デバイス）
２…ホストシステム（電子機器）
３…相手局（外部システム）
１０…赤外線通信部
１１…赤外線送信部
１２…赤外線受信部
２０…無線データ通信部
２１…アンテナ
２２…暗号化・復号化処理部
２３…送受信モジュール
３０…マイクロプロセッサ（ＣＰＵ）
３１…メモリ
５０…セルラー電話装置（携帯電話機）

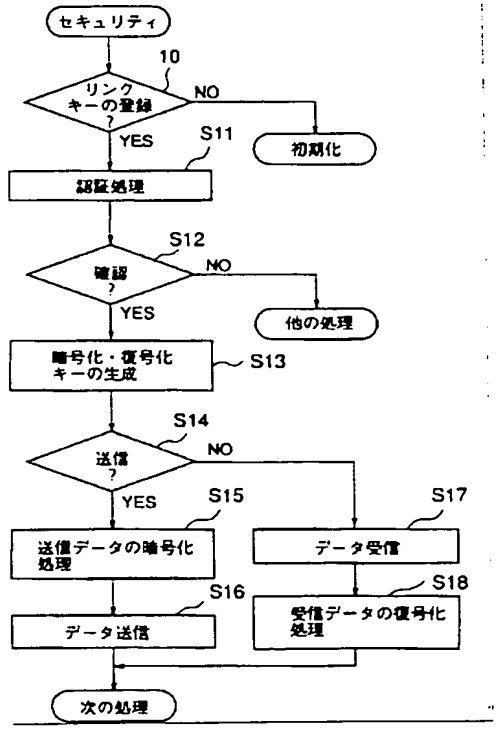
【図１】


31
30
1
11
10
3
メモリ
CPU
赤外線送信部
赤外線受信部
12
外部システム
22
ホスト
システム
暗号化・復号処理部
21
送受信モジュール
2
24
23
20

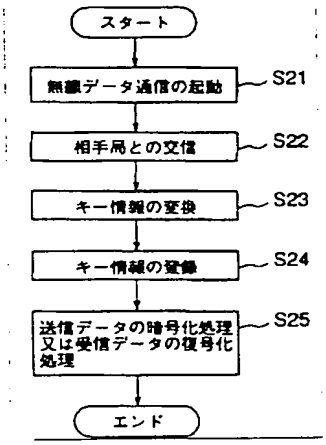
【図２】


スタート
属性の問い合わせ
S1
応答
?
NO
S2
YES
Ir通信
?
NO
S3
YES
呼び出し処理
S4
正常
?
NO
S5
YES
通信接続
他の処理

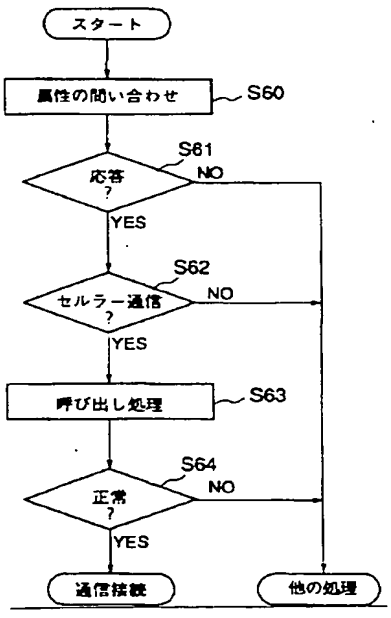
【図３】


セキュリティ
10
リンク
キーの登録
?
NO
YES
初期化
S11
認証処理
S12
確認
?
NO
YES
他の処理
暗号化・復号化
キーの生成
S13
S14
送信
?
NO
YES
S15
送信データの暗号化
処理
S17
データ受信
S16
データ送信
S18
受信データの復号化
処理
次の処理

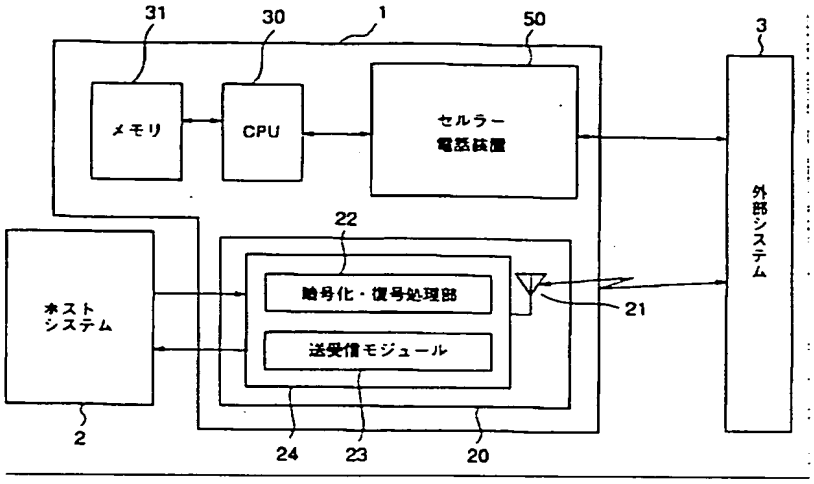
【図４】


スタート
無線データ通信の起動
S21
相手局との交信
S22
キー情報の交換
S23
キー情報の登録
S24
送信データの暗号化処理
又は受信データの復号化
処理
S25
エンド

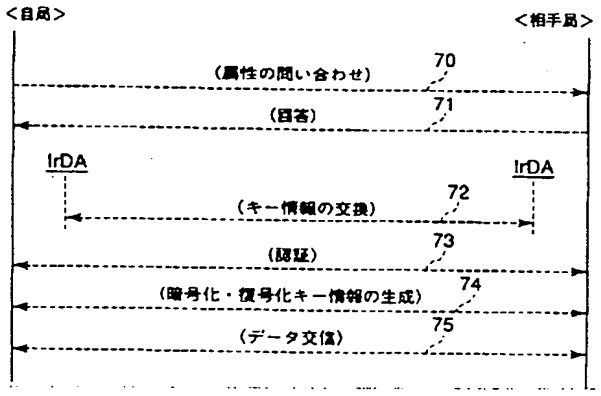
【図６】


スタート
属性の問い合わせ
S60
応答
?
NO
S61
YES
セルラー通信
?
NO
S62
YES
呼び出し処理
S63
正常
?
NO
S64
YES
通信接続
他の処理

【図５】



【図７】



フロントページの続き

(51) Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｑ 7/38			